CLAIMS

What is claimed is:

1. A method of providing a secure data stream between system nodes, the method comprising:

encrypting data at a node with an encryption key;

selecting encrypted data; and

regenerating a new encryption key at a node with an encryption key and selected encrypted data.

2. The method of claim 1 wherein the step of selecting encrypted data comprises selecting encrypted data using a byte from a previous encryption key as a seed of random generation.

3. The method of claim 1 wherein the step of regenerating a new encryption key comprises regenerating a new encryption key by performing a logic operation on a previous encryption key and selected encrypted data.

4. The method of claim 3 wherein the step of regenerating a new encryption key by performing a logic operation comprises regenerating a new encryption key by performing an XOR logic operation on a previous encryption key and selected encrypted data.

5. The method of claim 3 wherein the step of regenerating a new encryption key by performing a logic operation comprises performing a logic

operation on a previous encryption key and selected encrypted data to form an expanded key.

6. The method of claim 5 further comprising the step of selecting bytes from an expanded key to generate the new encryption key.

7. The method of claim 6 wherein the step of selecting bytes from an expanded key to generate the new encryption key comprises randomly selecting bytes from an expanded key to generate the new encryption key.

8. The method of claim 7 wherein the step of randomly selecting bytes from an expanded key to generate the new encryption key comprises randomly selecting bytes from an expanded key using a byte from a previous encryption key as a seed of random generation.

9. The method of claim 1 further comprising the step of encrypting data with a new encryption key.

10. The method of claim 9 wherein the step of encrypting data with a new encryption key comprises performing a logic operation on the data and new encryption key.

11. The method of claim 10 wherein the step of performing a logic operation on the data and new encryption key comprises performing an XOR operation on the data and new encryption key.

12. The method of claim 10 wherein the step of performing a logic operation on the data and new encryption key comprises forming a cipher.

13. The method of claim 12 further comprising the step of permuting portions of the cipher to form another cipher.

14. The method of claim 9 further comprising the step of transmitting encrypted data over a data stream.

15. The method of claim 14 further comprising the step of receiving encrypted data at a destination node.

16. The method of claim 15 further comprising the step of decrypting encrypted data at the destination node.

17. The method of claim 16 wherein the step of decrypting encrypted data comprises decrypting with a decryption key.

18. The method of claim 17 further comprising the step of regenerating a new decryption key using selected decrypted data and a previous decryption key.

19. A system for providing a secure data stream between a source programmable apparatus and a destination programmable apparatus, the system comprising:

a source programmable apparatus;

a data stream created by said source programmable apparatus;

means for encrypting data of said data stream with an encryption key; and

means for regenerating a new encryption key using selected previously encrypted data.

20. The system of claim 19 further comprising:

a destination programmable apparatus in electrical communication with said source programmable apparatus;

means for transmitting encrypted data to said destination programmable apparatus;

means for decrypting said encrypted data received at said destination programmable apparatus with a decryption key; and

means for regenerating a new decryption key using selected previously decrypted data.